UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/987,911	11/16/2001	Mark Crosbie	10012198	7932

7590 09/05/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/987,911	CROSBIE ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to June 16, 2006. Claims 1-19 are currently pending consideration.

Response to Arguments

2. Applicant's arguments filed June 16, 2006 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Moran (U.S. Patent 6,647,400), does not teach "reading events representing various types of system calls." This argument is not found persuasive. The CPA states that the intrusion detection system handles different "events" (column 8 lines 1-4) and uses evidence that is gathered to formulate an assessment of the possible attack (column 8 lines 1-5). These events, or calls to the system (system calls) are handled by the intrusion detection system, which is interpreted as reading the events, since it gathers information, analyzes, and forms an assessment of the event. Therefore, it is asserted that the CPA does teach "reading events representing various types of system calls."

Furthermore, the Applicant argues that the CPA does not teach, "routing an event to an appropriate template, the event having multiple parameters." This argument is not found persuasive. The CPA teaches using a rule set and an attack signature

database, which communicates with the event database to determine possible intrusions (column 8 lines 6-19). The rule set and attack signatures, are used to compare against the events' parameters. The parameters of the event are interpreted as the distinguishing features of the event that the rule set and/or signature database use to filter an event as a possible intrusion (column 8 lines 12-23). Therefore, it is asserted that the CPA does teach, "routing an event to an appropriate template, the event having multiple parameters."

Furthermore, the Applicant argues that the CPA does not teach, "filtering an event as either a possible intrusion based on the multiple parameters and either dropping the event or outputting the event." This argument is not found persuasive. The CPA teaches using a rule set and an attack signature database, which communicates with the event database to determine possible intrusions (column 8 lines 6-19). The rule set and attack signatures, are used to compare against the events' parameters. The parameters of the event are interpreted as the distinguishing features of the event that the rule set and/or signature database use to filter an event as a possible intrusion (column 8 lines 12-23). Then the Intrusion Detection System (IDS) can use the information to issue an alert (outputting the event) or not (dropping the event) (column 8 lines 33-35). Therefore, it is asserted that the CPA does teach, "filtering an event as either a possible intrusion based on the multiple parameters and either dropping the event or outputting the event."

Therefore, the rejection is respectfully maintained for the pending claims as given below.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Moran (U.S. Patent No. 6,647,400).

4. Regarding claim 1, Moran discloses:

reading events representing various types of system calls (column 7 line 65 – column 8 line 23, column 13 lines 26-42);

routing the event to an appropriate template, the event having multiple parameters (column 7 line 65 – column 8 line 23, column 14 lines 13-31);

filtering the event as either a possible intrusion based on the multiple parameters and either dropping the event or outputting the event (column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-59); and

creating an intrusion alert if an event is output from said filtering step (column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-59).

5. With respect to claim 7, Moran et al. disclose a method of detecting critical file changes, comprising:

reading events including encoded information representing system calls (column 7 line 65 – column 8 line 23, column 13 lines 26-42);

routing the event to an appropriate template based on the encoded information (column 7 line 65 – column 8 line 23, column 14 lines 13-31);

filtering the event as either a possible intrusion based on the encoded information and either dropping the event or outputting the event (column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-59); and

creating an intrusion alert of an event is output from said filtering step (column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-59).

6. With respect to claim 14, Moran et al. disclose a system for detecting critical file changes, comprising:

a processor (column 5 lines 26-42);

a memory storing instructions which, when executed by the processor, cause the processor to:

route events to an appropriate template (column 7 line 65 – column 8 line 23, column 14 lines 13-31);

wherein the event includes one or more parameters (column 11 lines 15-65, column 32 lines 48-59);

filter the event as either a possible intrusion based on one of the one or more parameters and either dropping the event or outputting the event (column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-59); and

create an intrusion alert if an event is output from the filter (column 8 lines 33-35, column 11 lines 15-65, column 32 lines 48-59).

7. With respect to claims 2,8, and 15, Moran et al. disclose a method, wherein said filtering step outputs an event if the parameters indicate that the permission bits on a file or directory were changed (column 9 lines 33-47).

8. With respect to claims 3,9, and 16, Moran et al. disclose a method, wherein said filtering step outputs an event if the parameters indicate that a file was opened for truncation (column 11 lines 15-48, column 31 lines 31-56).

9. With respect to claims 4,10, and 17 Moran et al. disclose a method, wherein said filtering step outputs an event if the parameters indicate that ownership or group ownership of a file has been changed (column 9 lines 33-47, column 31 lines 30-57).

10. With respect to claims 5,11, and 18, Moran et al. disclose a method, comprising a create step which outputs an alert message if a file was renamed including a file that was renamed and a new name that the file was renamed to (column 9 lines 33-47, column 30 lines 7-13).

11. With respect to claim 6,12, and 19, Moran et al. disclose a method, comprising configuring templates based on a list of files and directories to be included or excluded

based on whether the files and directories are considered unmodifiable (column 32 lines 60-67).

12. With respect to claim 13, Moran et al. disclose a computer-readable medium storing instructions which, when executed by a processor, cause the processor to implement the method steps of claim 1 (column 5 lines 26-42, column 7 line 65 – column 8 line 23, column 11 lines 15-65, column 13 lines 26-42, column 32 lines 48-59).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
08/29/2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

8/31/06